Cyber Network Defense Team - Service Catalog

Calendar Year: 2016 Service Update

Version 2.1

Updated on: 3/8/2016

Service	Description	Cost	Notes
Independent Security Assessment (ISA)	The comprehensive assessment is designed to provide a wide reaching analysis of the current state of logical cybersecurity controls within the organization (AKA AB 670 Information Security Assessment). The assessment provides an Asset inventory, Vulnerability Scan of systems, Compliance Assessment of one Firewall configuration, and a hardening assessment of up to 10 organizational baseline system image templates. [** Sample costs provided for planning purposes, actual costs to be calculated by CND based on agency provide information **].	**$ 42,259.32 a)** **$ 70,002.70 b)** **$ 120,986.87 c)** **** For cost estiamte, please contact CND**	*a) <= 500 systems* *b) 3000 systems* *c) 7500 systems* 1
Agency Vulnerability Assessment (AVA)	Perform an asset discovery scanand subsecquent Vulnerablity scan for accessible systems, and provide vulnerability reporting infomration and core remediation recomendations based on NIST compliance correlations. Scan includes discovery of up to 12 Class "C" IP ranges or equivelents. [** Costs based on sample pricing for 3000 assets; for actual pricing, please request a custom quote for a specific number of assets **]	**$ 22,354.66** **** For cost estiamte, please contact CND**	1
Health Sampling Assessment (HSA)	Analysts perform a system vulnerability assessment of upto 150 systems located on the same logical network segment and generate a comprehensive findings report. This service is recommended for agencies attempting to assess the effectiveness of current organizational security patching ahead of an audit, security assessment, or as part of the indpendent analyiss of a non-government delivered system(s).	**$ 9,608.30**	1

Firewall Configuration Assessment (FCA)	Analyst performs Firewall Analysis & Compliance Review on specified firewall / device. Analysis and analytics will address security configuration and best practices, manageability, access controls, change management compliance (rule traceability; documented change requests, etc...); identification of overlapping or redundant rules; identification of unused rules; review firewall architecture for appropriate zone implementation, segmentation, and intercommunication; access compliance with applicable state firewall compliance rules..	$	**9,671.40**	2
Website Configuration Vulnerability Scan (WCV)	An analysis of web site and the directly subordinate pages as accessed from the root or sub-site of the specified URL (e.g. www.acme.ca.gov includes www.acme.ca.gov/service, etc...). Analysis considers risk exposure regarding information disclosure, Structured Query Language Injection (SQLi) susceptibility, resistance to Cross-Site Scripting (XXS) vulnerability. The scan will not attempt to compromise the host through vulnerability exploitation. Scanning is conducted externally and internally to identify Access Control Lists and other security differnces from an "Insider Threat" perspective.	$	**9,842.92**	3
Network Traffic Anomally and Indicators of Compromise (NIC)	Acquisition of raw network traffic captures from client network. Traffic will be replayed against multiple Intrusion Detection System engines and traffic analysis tools to perform a best effort analysis for the presence of Indicators of Compromise (IoC). Traffic analysis results to be provided via formal report and metrics.	$	**13,489.05**	4

Hybrid Penetration Testing (HPT)	This multifacited service consists of several parts that include a asset vulnerability scan and analysis of all network connected systems within scope; network endpoint discovery service, and a hydrid penetration test (up to 5 days on site) designed to identify potentially at risk device and system configurations, default application installations, and compromise password proceedures. This service is intended to provide compliance with SAM 5330.1 and is sold based on the number of assets in the overall enterprise. Client is provided a (+/-) 5% varriance. [** Sample pricing assumes 3000 systems, for agency specific pricing, please contact us. **]	$	**63,191.88** **** For cost estiamte, please contact CND**	5
System Engineering and Support (SES)	This service is designed to provide an adhoc Infomraiton Technology Engineering and Best Practice deployment support solution in direct support of a unique client requirement. Since each client requirement is unique (Scope, architecture, and requirements), this solition requires direct soordination with a CND repersentative to determine if an appropriate engineer is available to your the agency needs. Support is bill in Daily (8 hour) increments.	$	**905.83**	
Active Directory Health Analysis (AHA)	Perform analysis of one Active Directory Forest or Domain (as applicable to customer) to evaluate the operations of the agencies Active Directory forest infrastructure based upon a series of established metrics and Best Business Practices (BBPs) that address forest health, replication services, directory supporting services, separation of duties, and logical access control implementation. Physical access to agencies Forest Domain Controller(s) must be provided by agency.	$	**25,821.81**	
Security Content Automation Protocol Baseline Image Analysis (BIA)	Perform analysis of logical controls related to NIST 800-53 compliance using the Security Content Automaton Protocol (SCAP) logical analysis tool for up to 10 systems less than 50 miles form CND HQ. Service includes the analysis, collection of results, correlation of results into actionable recommendations, and presentation of the report.	$	**5,298.57**	6

Incident Response Support Services (IRS)	This service is designed to provide an agency engaged in Incident Response (IR) Operations with 2 additional support personnel for a day with the appropriate goal related skillsets (as identified by the agency & within the CND capability set) to augument ongoing, long-term recovery operations. Due to the dynamic nature of IR recovery operaiotns, the agency may request in advance uniquely qualified team members be layer into differnt phases of the recovery efforts (e.g. Exchange Engineer on Days 1-2, Symantec Engineer on Days 3-5, etc...). Specality requirements must be negoatiated in advance. Service is billed at the daily rate.	**$**	**2,388.31**

Notes:

All previous pricing is superceeded by this updated Service Catalog. This catalog pricing repersents sample costs based on commonly requested quantities. Some services costs are dependent on system or device counts which may lower or raise these sample cost projections. Actual cost is reflected on the CND issued IAA and is based on the specified statement of work.

Previously issued IAA pricing is grandfathered for 30 days from date of catalog change. IAA received aftter the 30 day window require reissuance to reflect the updated costs and terms.

Scan service costs are based on general Endpoint numbers and provide a +/- 5% varience. Customers are encouraged to request a custom estimate for their specific needs to ensure the best cost avoidance. Customers should review their Active Directory, Asset inventories, and Non-Windows management tool to provide as accurate as possible asset estimate

1 - Assessment conducted from a single location with LAN/WAN connectivity adquate for the assessment of the target systems. Agency must comply with pre-scan configuration requirements to ensure maximum asset access. Scans are conducted as a best effort service. Systems not configured in accorance with prescan guidance or otherwise not available for scan during the pre-agreed upon scan period will not be included in the final results.

2 - Cost applies per configuration. HA pairs are considered two firewalls. Clients should assess only the primary firewall since pairs are directly replicated. Results may be provided using NIST, PCI, ISO, NERC standards as specified in customer request.

3 - Scan scope limited to Root and logical subordinate pages (e.g. www.acme.com and acme.com/a, etc..). Scanner is

configured to not crawl external site to the scanned host. Client will be required to provide user-level authentication credentials for sites with logon protections.

4 - Raw packet capture at network point of egress /ingress subject to 24 hours of total collection or a maximum total packet capture size of 1.5TB

5 - Pentests are billed based on the number of systems on the network (+/-) 5% varience. Test is designed to detect misconfigutations and other artechure flaws related to insecure IT operations. Test is limited to five days of onsite access and does not guarentee that all know and unknown risks will be identified in the time alloted. Client required to acknowledge risks associated with Penetration testing prior to engagement.

6 - Baseline image analysis does not cover all operating systems. Customers are encouraged to request supported operating systems.